

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003 年 10 月 23 日 (23.10.2003)

PCT

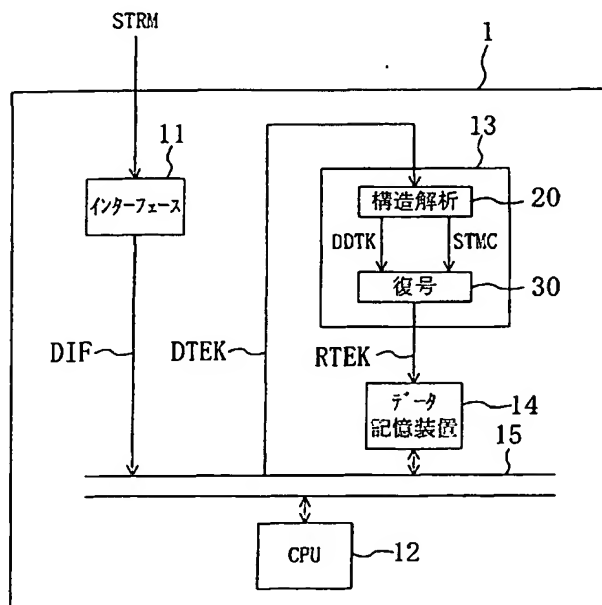
(10) 国際公開番号
WO 03/088557 A1

- (51) 国際特許分類: H04L 9/00, G09C 1/00, G06F 12/14 (72) 発明者; および
(75) 発明者/出願人 (米国についてののみ): 和田 妙美 (WADA, Taemi) [JP/JP]; 〒572-0013 大阪府 寝屋川市 三井が丘 4-4-8 2-4 0 6 Osaka (JP). 福岡 俊彦 (FUKUOKA, Toshihiko) [JP/JP]; 〒575-0061 大阪府 四 条 畹市 清滝中町 1 5-2 4 Osaka (JP).
- (21) 国際出願番号: PCT/JP03/04864
- (22) 国際出願日: 2003 年 4 月 16 日 (16.04.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ: 特願2002-114076 2002 年 4 月 17 日 (17.04.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電 器産業株式会社 (MATSUSHITA ELECTRIC INDUS- TRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真 1 0 0 6 番地 Osaka (JP).
- (74) 代理人: 前田 弘, 外 (MAEDA, Hiroshi et al.); 〒550- 0004 大阪府 大阪市 西区鞠本町 1 丁目 4 番 8 号 本町 中島ビル Osaka (JP).
- (81) 指定国 (国内): CN, KR, US.
- (84) 指定国 (広域): ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR).

[続葉有]

(54) Title: DIGITAL TWO-WAY COMMUNICATION CONTROL DEVICE AND ITS METHOD

(54) 発明の名称: デジタル双方向通信制御装置およびその方法



11...INTERFACE
20...STRUCTURAL ANALYSIS
30...DECODING
14...DATA STORAGE DEVICE

(57) Abstract: An interface block (11) converts the format of received downstream data (STRM). On receiving the format-converted data (DIF), a CPU (12) executes the MAC function. On receiving TEK processing data (DTEK) obtained from the data (DIF), a TEK processing block (13) analyzes the data structure and, according to the analysis result, decodes the data.

(57) 要約: インターフェースブロック (11) は、入力されたダウンストリームデータ (STRM) をフォーマット変換する。CPU (12) はフォーマット変換されたデータ (DIF) を受けて、MAC機能を実現する。またTEK処理ブロック (13) はデータ (DIF) から得られたTEK処理データ (DTEK) を受け、そのデータ構造の解析を行い、この解析結果を基にして復号処理を行う。



添付公開書類:
— 国際調査報告書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明細書

デジタル双方向通信制御装置およびその方法

技術分野

本発明は、デジタル双方向通信における双方向制御を行う装置に関するものであり、特に、センター装置側から端末装置側への下り方向通信に係る構成の最適化を行う技術に属する。

背景技術

双方向CATVに代表されるデジタル双方向通信システムは、センター装置に対して複数の端末装置が接続された双方向通信網によって構成されている。この個々の端末装置において、センター装置側から端末装置側への下り方向通信および端末装置側からセンター装置側への上り方向通信の双方向制御はMAC (Media Access Control) 機能と呼ばれ、通常は、通信データ中にサブレイヤーとして埋め込まれたMAC特有の構造をもつプロトコルの解読によって、処理機能が実現される。

MAC構造の一例として、MCNS (Multimedia Cable Network Systems partners) という米国のケーブルオペレータやケーブルTVセットのサプライヤーからなる団体によって提唱され、現在ではデファクトスタンダードとなっているDOCSIS (Data Over Cable Service Interface Specifications) 方式が存在する。その詳細については、米国のCable Labs (Cable Television Laboratories Inc.) が提供している仕様書「Data-Over-Cable Service Interface Specifications」の「Radio Frequency Interface Specification SP-RF1v1.1-106-001215」に開示されている。

下り方向通信では、通常、主として映像データが送信される。したがって、通信データはMPEG構造を有しているが、そのサブレイヤーとしてMAC構造が定義されている。下り方向通信は比較的広い帯域に通信チャネル周波数が割り当てられるため、通信制御自体は比較的単純であるが、映像データが送信されるた

めに膨大なデータ量を取り扱う必要があり、決められた手順に従って、リアルタイムに、誤り無く処理することが要求される。

一方、上り方向通信では、通常、主として制御データが送信される。この制御データには、端末装置側からの命令要求や、端末装置各々の状態を知らせるためのステート表示データが含まれる。上り方向通信において送信される制御データを受けて、センター装置側は、各端末装置の要求命令に応えたり、端末装置を正しく制御するための各種情報を下り方向通信の制御データとして送信したりする。上り方向通信は、狭い帯域に多数の通信チャネル周波数が割り当てられるため、複数の端末装置間で衝突が生じたり、必要な通信チャネル周波数が得られない場合が生じるなど、一般に複雑な制御が必要であり、その機能は双方向通信における通信性能に大きな影響を与える。

DOCSIS MAC構造は、イーサネットによるIP通信との親和性を高めるため、基本的にイーサネット通信と同様の構造を有しているが、DOCSIS特有の領域としての各種ヘッダフィールドを設けている。その中でも、「拡張ヘッダ」と呼ばれる可変長領域のフィールドによって、暗号その他の付加機能が定義されることが特徴である。

MAC機能の実現には、上記仕様書に示されているように、複雑な多層構造を有するデータ構造を解析した後に、各種処理を適切なタイミングで行うことが必要となる。多数の処理を、膨大な数に上る組合せについて実現すること、そして、その組合せ動作の正しさを検証することは、非常に難度が高く、処理量が非常に多い。

次に各処理の内容に着目すると、MAC機能を構成する個々の処理は制御系の演算処理が主であり、基本的に、データのフィルタリング（振り分け）、同期処理、並び替え、フォーマット化等の個々の処理およびその組合せである。これらの個々の処理自体は、決して負荷の大きい処理とはいえない。

しかしながら、MAC機能には、通信システムには不可欠なデータのセキュリティ機能が含まれており、DOCSIS方式に関しては、その詳細仕様が、米国のCable Labsから出された仕様書「Data-Over-Cable Service Interface Specifications」の「Baseline Privacy Plus Interface Specifications SP-

BPI+ -106-001215」に開示されている。

MAC機能のセキュリティ機能は、Baseline Privacyといい、BPKM (Baseline Privacy key Management) と呼ばれるプロトコルを使用する。BPKMでは、安全な鍵交換を行なうため、暗号鍵自体を暗号化してやり取りする機能や、暗号鍵交換のメッセージが正しい相手から送信されたことや、改ざんされていないことを確認するためのメッセージ認証機能を備えている。BPKMではマスターキーとなるAuthorization Keyと、実際にデータの暗号化および復号化に使用するDES暗号キー (Traffic Encryption Key、TEKという呼ぶ) という二段階の鍵を使用して鍵の配布を行なう。

端末装置はRSA公開鍵方式で暗号化されたAuthorization Keyを受け取り、RSA公開鍵を用いて、このAuthorization Keyを復号する。次に、取得したAuthorization KeyからTEKの復号化や認証を行ういくつかの処理を経てTEKデータを取得し、最終的にこのTEKデータを用いて、実際の通信データの復号化を行なう。ここで、Authorization Keyの復号化を行うRSA暗号の復号処理や、TEKデータの復号化を行うDES暗号の復号化についても、64ビット単位のデータを複数用いた数値演算が並列にかつ繰り返し必要となることから、個々の処理も相当に負荷の大きい処理といえる。

デジタル双方向通信における双方向制御を行うMAC機能を実現するためには、このような処理を組み合わせる必要があるとされている。

－解決課題－

MAC機能は、汎用プロセッサ (CPU) を用いて実現することが一般的である。これは、CPUには複雑な処理に対して柔軟に対応できる利点があり、システムの信頼性を確立するための検証や機能修正も比較的容易に実現できるからである。

ところが、MAC機能は、その膨大な処理を実現するために、高性能なCPUを用いなければならないことは必須である。また、単にCPUを占有するにとどまらず、単一のCPUでは所望の全機能を実現することは極めて困難になっている。このため、MAC機能を全て実現する装置を構成するためには、回路規模が格段に大きくなり、非現実的なほどコストの高い装置となってしまう。

前記の問題に鑑み、本発明は、デジタル双方向通信制御において、CPU処理の負荷軽減を図り、装置全体の回路規模の適正化を実現することを課題とする。

発明の開示

本発明は、デジタル双方向通信における双方向制御を行う装置として、入力されたダウンストリームデータをフォーマット変換して下り方向データを生成するインターフェースブロックと、前記下り方向データを受けてMAC (Media Access Control) 機能を実現するCPUと、前記下り方向データから得られたTEK (Traffic Encryption Key) 処理データを受け、そのデータ構造の解析を行い、この解析結果を基にして復号処理を行うTEK処理ブロックとを備えたものである。

これにより、MAC機能を実現するための処理のうち、TEK処理データの構造解析と、この解析結果を基にした復号処理とが、CPUとは別個のTEK処理ブロックによって行われる。このため、CPU処理の負荷が軽減され、装置全体を、適正な回路規模によって構成することが可能になる。

そして、前記本発明に係るデジタル双方向通信制御装置におけるTEK処理ブロックは、TEK処理データを入力し、このTEK処理データの中のMPEG構造とMPEG構造に埋め込まれたMAC (Media Access Control) 構造とを解析し、MAC構造を持つデータであるMACデータの状態および意味を示すMACステート情報データを出力する構造解析ブロックと、TEK処理データ中の暗号化された部分を前記MACステート情報データを参照して判別し、暗号化された部分を暗号を解くためのTEKデータを用いて復号し、その復号結果を暗号化されていない部分と統合する復号ブロックとを備えているのが好ましい。

そして、前記本発明に係るデジタル双方向通信制御装置における構造解析ブロックは、TEK処理データ中のMPEG構造のヘッダであるMPEGヘッダを解析し、MACデータの位置を示すMACデータ位置信号、およびMACフレームの先頭バイト位置を示すMACデータ先頭位置信号を出力するMPEGヘッダ解析ブロックと、前記MACデータ位置信号およびMACデータ先頭位置信号を入力とし、MAC構造のヘッダであるMACヘッダ中の拡張ヘッダおよびMACM

M (MAC Management Message) ヘッダ以外のフィールドについてステート情報を認識するとともに、TEK処理データに拡張ヘッダが存在するとき拡張ヘッダの位置を示す拡張ヘッダ位置情報データを出力し、かつ、TEK処理データにMACMMヘッダが存在するときMACMMヘッダの位置を示すMACMMヘッダ位置情報データを出力するMACヘッダ解析ブロックと、前記拡張ヘッダ位置情報データを受けて拡張ヘッダの各フィールドをチェックし、拡張ヘッダのステート情報を示す拡張ヘッダステート情報データを出力する拡張ヘッダ解析ブロックと、前記MACMMヘッダ位置情報データを受けてMACMMヘッダの各フィールドをチェックし、MACMMヘッダのステート情報を示すMACMMヘッダステート情報データを出力するMACMMヘッダ解析ブロックとを備え、前記MACヘッダ解析ブロックは、前記拡張ヘッダステート情報データおよびMACMMヘッダステート情報データを受け、MACヘッダ中の拡張ヘッダおよびMACMMヘッダ以外の各フィールドのステート情報と、前記拡張ヘッダステート情報データが示す拡張ヘッダのステート情報および前記MACMMヘッダステート情報データが示すMACMMヘッダのステート情報とを基にして、前記MACステート情報データを生成するものとするのが好ましい。

さらに、前記MPEGヘッダ解析ブロックは、MPEGヘッダのフィールドをチェックして、MACデータの位置とMACフレームの先頭バイト位置とを検出し、前記MACデータ位置信号およびMACデータ先頭位置信号を出力するのが好ましい。

または、前記MACヘッダ解析ブロックは、HCSチェックによって、MACヘッダの誤り検出を行うのが好ましい。あるいは、前記MACヘッダ解析ブロックは、MACヘッダの中のMACデータ長を示すフィールドのチェックを行うものであり、前記チェックを、前記MACデータ先頭位置信号を参照してMACフレームのデータ長をカウントし、このMACフレーム長が、当該フィールドの値と所定のデータ長との和と一致するか否かを判断することによって、行うのが好ましい。あるいは、前記MACヘッダ解析ブロックは、HCSチェックに加えて、MACフレーム長チェックおよび拡張ヘッダ長チェックによって、MACヘッダの誤り検出を行うものであり、かつ、前記MACフレーム長チェックおよび拡張

ヘッダ長チェックによるチェック結果が、エラーなしであるとき、前記HCSチェックによるチェック結果を無効にするのが好ましい。

または、前記拡張ヘッダ解析ブロックは、前記拡張ヘッダ位置情報データを参照して拡張ヘッダのフィールドをチェックし、拡張ヘッダのデータ長や種類を判別し、拡張ヘッダのフィールドの値が不当である場合、拡張ヘッダに誤りがあると認識し、その旨を前記拡張ヘッダステート情報データとして出力するのが好ましい。

または、前記MACMMヘッダ解析ブロックは、前記MACMMヘッダ位置情報データを参照してMACMMヘッダのフィールドをチェックし、MACMMのデータ長および種類を判別し、MACMMヘッダのフィールドのデータの値が不当である場合、MACMMヘッダに誤りがあると認識し、その旨を前記MACMMヘッダステート情報データとして出力するのが好ましい。

また、前記本発明に係るデジタル双方向通信制御装置における復号ブロックは、前記MACステート情報データを参照して、TEK処理データ中の暗号化された部分と暗号化されていない部分とを選別し、TEK処理データからTEKデータを選択するためのTEK照合データを抽出し、抽出したTEK照合データを参照して、予め保持していた複数のTEKデータの中から、復号に用いるTEKデータを選択し、暗号化された部分を復号処理単位のビット幅に変換し、選択したTEKデータを用いて復号し、復号後のデータと暗号化されていない部分とを統合するのが好ましい。

また、本発明は、デジタル双方向通信における双方向制御を行う方法として、入力されたダウンストリームデータをフォーマット変換して下り方向データを生成するステップと、CPUによって、前記下り方向データを受けてMAC(Media Access Control)機能を実現するステップと、TEL処理ブロックによって、前記下り方向データから得られたTEK(Traffic Encryption Key)処理データを受け、そのデータ構造の解析を行い、この解析結果を基にして、復号処理を行うTEK処理ステップとを備えたものである。

そして、前記本発明に係るデジタル双方向通信制御方法におけるTEK処理ステップは、TEK処理データの中のMPEG構造とMPEG構造に埋め込まれた

MAC (Media Access Control) 構造とを解析し、MAC 構造を持つデータである MAC データの状態および意味を示す MAC ステート情報データを生成する構造解析ステップと、TEK 処理データ中の暗号化された部分を前記 MAC ステート情報データを参照して判別し、暗号化された部分を暗号を解くための TEK データを用いて復号し、その復号結果を暗号化されていない部分と統合する復号ステップとを備えているのが好ましい。

そして、前記構造解析ステップは、TEK 処理データの MPEG 構造のヘッダである MPEG ヘッダを解析し、MAC データの位置を示す MAC データ位置信号、および MAC フレームの先頭バイト位置を示す MAC データ先頭位置信号を生成する MPEG ヘッダ解析ステップと、前記 MAC データ位置信号および MAC データ先頭位置信号を用い、MAC 構造のヘッダである MAC ヘッダ中の拡張ヘッダおよび MAC MM (MAC Management Message) ヘッダ以外のフィールドについてステート情報を認識するとともに、TEK 処理データに拡張ヘッダが存在するとき拡張ヘッダの位置を示す拡張ヘッダ位置情報データを生成し、かつ、TEK 処理データに MAC MM ヘッダが存在するとき MAC MM ヘッダの位置を示す MAC MM ヘッダ位置情報データを生成する MAC ヘッダ解析ステップと、前記拡張ヘッダ位置情報データを受けて拡張ヘッダの各フィールドをチェックし、拡張ヘッダのステート情報を示す拡張ヘッダステート情報データを生成する拡張ヘッダ解析ステップと、MAC MM ヘッダ位置情報データを受けて MAC MM ヘッダの各フィールドをチェックし、MAC MM ヘッダのステート情報を示す MAC MM ヘッダステート情報データを生成する MAC MM ヘッダ解析ステップとを備え、前記 MAC ヘッダ解析ステップにおいて判断した、MAC ヘッダ中の拡張ヘッダおよび MAC MM ヘッダ以外の各フィールドのステート情報と、前記拡張ヘッダステート情報データが示す拡張ヘッダのステート情報、および前記 MAC MM ヘッダステート情報データが示す MAC MM ヘッダのステート情報とを基にして、前記 MAC ステート情報データを生成するものとするのが好ましい。

図面の簡単な説明

図 1 は本発明の一実施形態に係るデジタル双方向通信制御装置の構成を示すブ

ロック図である。

図 2 は図 1 に示す構造解析ブロックの内部構成を示す図である。

図 3 は本発明の一実施形態に係る M P E G ヘッダ解析のステートマシンを示す図である。

図 4 は M P E G ヘッダのフォーマットを示す図である。

図 5 はポインタフィールドを含む M P E G データのフォーマットを示す図である。

図 6 は本発明の一実施形態に係る M A C ヘッダ解析のステートマシンである。

図 7 は M A C データのフォーマットを示す図である。

図 8 は H C S チェック以外の M A C ヘッダ誤り検出方法を説明するための図である。

図 9 は本発明の一実施形態に係る拡張ヘッダ解析のステートマシンである。

図 1 0 は拡張ヘッダのフォーマットを示す図である。

図 1 1 は拡張ヘッダの一例 (Downstream Privacy) のフォーマットを示す図である。

図 1 2 は本発明の一実施形態に係る M A C M M ヘッダ解析のステートマシンである。

図 1 3 は M A C M M ヘッダのフォーマットを示す図である。

図 1 4 は本発明の一実施形態に係る復号ブロックの動作を示すフローチャートである。

発明を実施するための最良の形態

以下、本発明の実施形態について、図面を参照しながら説明する。

図 1 は本発明の一実施形態に係るデジタル双方向通信制御装置の構成を示すブロック図である。図 1 に示すデジタル双方向通信制御装置 1 は、センター装置および複数の端末装置によって構成される双方向通信網において双方向通信制御を行うものであり、端末装置の内部に設けられる。

図 1 において、1 1 はセンター装置側から送信される映像および伝送制御データであるダウンストリームデータ S T R M を入力とし、C P U 1 2 へ送るために

フォーマット変換して、下り方向データとしてのCPUインターフェースデータDIFを生成するインターフェースブロック、12はCPUインターフェースデータDIFをCPUバス15を介して受け、MAC(Media Access Control)機能を実現するCPU、14はCPUバス15を介してCPU12とデータのやり取りを行うデータ記憶装置である。

また13は映像および伝送制御データのうちTEK処理に用いられるデータであるTEK処理データDTEKを入力とし、データ構造の解析、暗号化の有無の確認、データの復号およびデータ変換を行い、当該処理の結果をTEK処理結果データRTEKとして出力するTEK処理ブロックである。TEK処理ブロック13は、TEK処理データDTEKの構造解析を行い、遅延TEK処理データDDTKおよびMACステート情報データSTMCを出力する構造解析ブロック20と、遅延TEK処理データDDTKとMACステート情報データSTMCを用いて、遅延TEK処理データDDTKにおける暗号化の有無の判別、復号処理およびデータのビット変換を行い、TEK処理結果データRTEKを出力する復号ブロック30とを備えている。TEK処理ブロック13から出力されたTEK処理結果データRTEKは、データ記憶装置14に入力される。

ここで、MACステート情報データSTMCは、TEK処理データDTEK中のMPEG構造に埋め込まれた、ネットワーク処理用のサブレイヤであるMAC構造を持つデータ(MACデータ)の状態および意味を示すものである。また遅延TEK処理データDDTKは、MACステート情報データSTMCと時間的に対応付けるために、TEK処理データDTEKを0または1クロック以上遅延させたものである。さらに、CPUインターフェースデータDIFは、ダウンストリームデータSTRMをフォーマット変換した結果のデータの他に、CPUバス15の制御信号を含んでいる。

図1に示すデジタル双方向通信制御装置1の動作について、説明する。

端末装置は、ダウンストリームデータSTRMを受信すると、これをデジタル双方向通信制御装置1内のインターフェースブロック11に送る。インターフェースブロック11はダウンストリームデータSTRMのフォーマットを変換し、CPUインターフェースデータDIFとして出力する。CPU12はCPUバス

15を介してCPUインターフェースデータDIFを受けて、データ記憶装置14とともに、MAC機能を実現するためのさまざまな処理を行う。ただし、MAC機能のうちTEK処理に用いられるデータであるTEK処理データDTEKは、CPU12からCPUバス15を介してTEK処理ブロック13に送られる。

TEK処理ブロック13では、TEK処理データDTEKが入力されると、まず構造解析ブロック20が、TEK処理データDTEKにおけるMPEG構造とMPEG構造に埋め込まれているMAC構造との構造解析を行う。構造解析ブロック20から出力された遅延TEK処理データDDTKおよびMACステート情報データSTMCは復号ブロック30に送られる。復号ブロック30は、遅延TEK処理データDDTKにおける、データの機密性保護のためセンター装置側でDES (Data Encryption Standard) により暗号化されたデータについて復号処理を行い、データ記憶装置14にTEK処理結果データRTEKを出力する。構造解析ブロック20と復号ブロック30における処理の詳細については、後述する。

このような構成によって、MAC機能を実現するための処理のうち、TEK処理データDTEKの構造解析と、この解析結果を基にした復号処理とが、CPU12とは別個のTEK処理ブロック13によって行われる。このため、CPU処理の負荷が大幅に軽減される。また、TEK処理ブロック13における処理は、そのほとんどが、同じような数値演算を並列にかつ繰り返し実行することによって実現されるので、ハード構成も簡易なものになる。したがって、装置全体を、適正な回路規模によって構成することが可能になる。

なお、TEK処理データDTEKをCPUバス15からTEK処理ブロック13に送るパスを双方向にすることによって、TEK処理の一部をCPU12によって実行することが可能になる。また、インターフェースブロック11からTEK処理ブロック13に直接、映像および制御データを送ることによって、CPUバス15の占有率を下げることもできるとともに、CPU処理の高速化を図ることが可能になる。また、ダウンストリームデータSTRMの入力パスと、インターフェースブロック11からCPUバス15へのCPUインターフェースデータDIFのパスを、それぞれ双方向にすることによって、双方向通信制御が可能と

なる。

＜構造解析ブロック＞

図2は図1に示す構造解析ブロック20の内部構成を示すブロック図である。図2において、21はTEK処理データDTEK中のMPEG構造のヘッダであるMPEGヘッダを解析し、MPEG構造からMAC構造を抜き出し、MACデータのデータ位置を示すMACデータ位置信号PMC、MACフレームの先頭バイト位置を示すMACデータ先頭位置信号LPMCを出力するMPEGヘッダ解析ブロックである。MPEGヘッダ解析ブロック21は、TEK処理データDTEKを遅延させて得た遅延TEK処理データDDTKとともに、これに係るMACデータ位置信号PMCおよびMACデータ先頭位置信号LPMCを出力する。

22はMACデータ位置信号PMCおよびMACデータ先頭位置信号LPMCを入力とし、MAC構造を有するMACデータ中のヘッダ部分（MACヘッダ）中の、拡張ヘッダとMACMM（MAC Management Message）ヘッダ以外の部分について解析を行い、各フィールドのステート情報すなわちデータの意味を判断するMACヘッダ解析ブロックである。またMACヘッダ解析ブロック22は、遅延TEK処理データDDTKに拡張ヘッダが存在するとき、拡張ヘッダの位置を示す拡張ヘッダ位置情報データPEHを出力し、かつ、遅延TEK処理データDDTKにMACMMヘッダが存在するとき、MACMMヘッダの位置を示すMACMMヘッダ位置情報データPMMを出力する。

また、23は拡張ヘッダ位置情報データPEHを受けて、MACヘッダ中の拡張ヘッダの解析を行い、拡張ヘッダのステート情報すなわち状態、意味を示す拡張ヘッダステート情報データSTEHを出力する拡張ヘッダ解析ブロック、24はMACMMヘッダ位置情報データPMMを受けて、MACMMヘッダの解析を行い、MACMMヘッダのステート情報すなわち状態、意味を示すMACMMヘッダステート情報データSTMMを出力するMACMMヘッダ解析ブロックである。

そして、MACヘッダ解析ブロック22は、拡張ヘッダステート情報データSTEHおよびMACMMヘッダステート情報STMMを受け、MACヘッダ中の拡張ヘッダおよびMACMMヘッダ以外のフィールドのステート情報と、拡張ヘ

ッダステート情報データSTE Hが示す拡張ヘッダのステート情報およびMAC MMヘッダステート情報STM Mが示すMAC MMヘッダのステート情報とを基にして、MACステート情報データSTMCを生成する。

各解析ブロック21～24の動作について、さらに詳細に説明する。

＜MPEGヘッダ解析＞

MPEGヘッダ解析ブロック21は、TEK処理データDTEK中のMPEGヘッダを解析することによって、MPEG構造からMAC構造を抜き出す。具体的には、MPEGヘッダの各フィールドを逐次チェックし、各フィールドのデータの意味を判断し、データにステートを与える。

図3はMPEGヘッダ解析ブロック21におけるMPEGヘッダ解析のステートマシンを示す図である。また図4はMPEGヘッダのフォーマットを示す図である。図3に従って、MPEGヘッダ解析における処理の流れを説明する。

ステートマシンのステートはバイトクロック毎に遷移する。ステートの初期状態は「IDLE」であり、TEK処理データDTEKに誤りがある場合は、ステートを「ERR」にする。

ステートが「IDLE」であるとき、TEK処理データDTEKに含まれるパケットシンクがMPEGフレームの先頭を示すまで、そのステートを保持する（S11）。そして、パケットシンクがMPEGフレームの先頭を示したとき、MPEGデータの先頭データ、すなわち図4に示すMPEGパケットシンクバイトデータ（sync byte）の値が“0x47”であるとき、ステートを「S1」にする（S12）。一方、そうでないときはステートを「ERR」にする。

ステートが「S1」であるとき、図4に示すTEI（Transport Error Indicator）データの値が“0x0”であり（S13）、かつ、図4に示すPID（Program ID）の上位5ビットの値が“0x1F”である（S14）とき、ステートを「S2」にし、そうでないときはステートを「ERR」にする。TEIデータはMPEG構造に誤りがあるか否かを示すものであり、誤り訂正処理時に付加される。また、PIDはDOCSIS仕様のMACフレームを転送するMPEGデータに設定されている。

ステートが「S2」であるとき、PIDの下位8ビットの値が“0xFE”で

ある場合は、ステートを「S 3」にし、そうでないときはステートを「ERR」にする（S 15）。そしてステートが「S 3」であるとき、図4に示すトランスポートスクランブルコントロールデータ（Transport scrambling control）の値が“0 x 0”であり、かつ、図4に示すアダプテーションフィールドコントロールデータ（Adaptation field control）の値が“0 x 1”であるとき、ステートを「S 4」にし、そうでないときはステートを「ERR」にする（S 16）。トランスポートスクランブルコントロールデータはスクランブル制御に関するコントロールデータであり、アダプテーションフィールドコントロールデータはDOCSIS用フィールド割り当てコントロールデータである。

ステートが「S 4」である場合、図4に示すPUSI（payload unit start indicator）の値が“0 x 1”のとき、ポインタフィールドが存在すると判断し、ステートを「POINTER」にする（S 17）。そうでないときは、ステートを「MAC_FRM」にする。PUSIはMPEGデータにMACデータの先頭が存在するか否かを示すものである。ここで、ポインタフィールドは、MACデータ先頭位置信号LPMCを生成する際に重要となるデータであり、詳細については後述する。

ステートが「MAC_FRM」であるとき、MPEGパケットシンクバイトデータが現れるまでステートを保持し（S 18）、MPEGパケットシンクバイトデータが現れ、かつ、その値が“0 x 4 7”である場合（S 12）、ステートを「S 1」にし、そうでないときはステートを「ERR」にする。

一方、ステートが「ERR」であるとき、パケットシンクがMPEGデータの先頭を示すまでステートを保持し（S 19）、パケットシンクがMPEGデータの先頭を示したとき、MPEGパケットシンクバイトデータの値が“0 x 4 7”である場合には、ステートを「S 1」にし（S 12）、そうでないときはステートを保持する。

ここで、図5を用いて、ポインタフィールドと、MACデータ先頭位置信号LPMCおよびMACデータ位置信号PMCの生成方法について説明する。図5はポインタフィールドを含むMPEGデータのフォーマットを概念的に示す図であり、図5に示すようなMPEGデータはTEK処理データDTEKに含まれてい

る。

図5では、MPEGヘッダにおけるPUSIの値が“0x1”であり、ポインタフィールドがあることを示している。そして、MPEGヘッダの後ろにポインタフィールドが存在しており、そのポインタフィールドの値がM（M：整数）になっている。これは、ポインタフィールドの後ろに、一のMACフレーム（MAC Frame #1）の残りのデータがMバイト存在し、その次から新たなMACフレーム（MAC Frame #2）が始まることを示している。したがって、ポインタフィールドの値Mから、MACフレームの先頭バイト位置を検出することが可能になる。

すなわち、ステートが「POINTER」であるデータがポインタフィールドであることから、ポインタフィールドカウンタを設けて、このポインタフィールドカウンタによって、ステートが「POINTER」である位置すなわちポインタフィールドの位置からカウントを行う。そして、このポインタフィールドカウンタによるカウンタ値がポインタフィールドの値と等しくなったとき、その位置がMACフレームの先頭バイト位置であると認識する。これにより、MACデータ先頭位置信号LPMCを生成する。

また、ステートが「MAC_FRM」である間のデータはMAC構造であることから、これに従って、MACデータ位置信号PMCを生成する。図5では、MPEGデータと、MACデータ先頭位置信号LPMCおよびMACデータ位置信号PMCとの関係を概念的に示している。

なお、ここで求めた各フィールドのステート情報はレジスタに保持する。そして、TEK処理データとステート情報とを対応づけるために、TEK処理データDTEKを0または1クロック以上遅延させて、遅延TEK処理データDDTKを生成する。

なお、MPEG構造の保護機能について、TEIデータに対する前方保護および後方保護カウンタを設けるだけでなく、MPEG構造データ長（188バイト）をカウントするMPEGフレーム長カウンタを設け、TEIデータがエラーを示していない場合でも、次のMPEG構造の先頭データまでのMPEG構造データ長が188でない場合は、そのMPEG構造はエラーであると判断する機能を設けることは可能である。

＜MACヘッダ解析＞

MACヘッダ解析ブロック22は、遅延TEK処理データDDTKの中のMACヘッダの解析を行う。具体的には、MACヘッダの各フィールドを逐次チェックし、各フィールドのデータの意味を判断し、データにステートを与える。

図6はMACヘッダ解析ブロック22におけるMACヘッダ解析のステートマシンを示す図である。このMACヘッダ解析のステートマシンは、MACデータ位置信号PMCが有効であるときのみ、動作する。また図7はMACデータのフォーマットを示す図である。図6に従って、MACヘッダ解析における処理の流れを説明する。

ステートマシンのステートはバイトクロック毎に遷移する。ステートの初期状態は「IDLE」であり、MAC構造に誤りがある場合はステートを「ERR」にする。

ステートが「IDLE」であるとき、MACデータ先頭位置信号LPMCが、有効でないときはそのステートを保持し、有効であるときはステートを「FC」にする（S21）。ここで、ステートが「FC」であるときのMACヘッダは、FC（Field Control）データであり、MACデータの種類や、MACデータの構成の拡張を可能にする拡張ヘッダの有無を示す。

ステートが「FC」であるとき、FCデータの値を解析する（S22）。そしてFCデータの値が、SYNCデータを示す場合はステートを「PARM_T」にし（S22A）、MACMMを示す場合はステートを「PARM_M」にし（S22B）、PacketPDUを示す場合はステートを「PARM_D」にする（S22C）。また、FCデータの値が0xffであり、MPEG構造データのダミーデータであるSTUFFバイトを示す場合はステートを保持し（S22D）、FCデータがそれ以外の場合はステートを「ERR」にする（S22E）。なお、SYNCデータは、センタ装置側から送信される、同期処理に必要なデータを転送するためのMAC構造であり、MACMMは、センタ装置側から送信される、MACの制御に用いる帯域割り当てデータや同期処理に必要なデータなどを転送するためのMAC構造であり、PacketPDUは、通常の映像データを転送するためのMAC構造である。

また、FCデータに含まれたEHDR_ONの値から、MACデータ中の拡張ヘッダの有無を判別する。“0”のときは拡張ヘッダが存在せず、“1”のときは拡張ヘッダは存在する。

ステートが「PARM_T」「PARM_M」「PARM_D」であるとき、ステートを「LEN_H」にする。ステートが「LEN_H」であるとき、ステートを「LEN_L」にする。ステートが「LEN_L」であるとき、EHDR_ONの値から拡張ヘッダの有無を判断する（S23）。拡張ヘッダが存在するときはステートを「EHDR」にし、そうでないときはステートを「HCS_H」にする。

ステートが「EHDR」である期間は、拡張ヘッダの位置であるため、拡張ヘッダ位置情報データPEHを生成し、これを遅延TEK処理データDDTKとともに拡張ヘッダ解析ブロック23へ送る。拡張ヘッダ解析ブロック23の処理内容については、後述する。

ステートが「EHDR」であるとき、拡張ヘッダ解析ブロック23の処理が行われている間はステートを保持する。そして、拡張ヘッダ解析ブロック23から出力された拡張ヘッダステート情報データSTEHから、拡張ヘッダ解析処理が正常に終了したことを確認したとき、ステートを「HCS_H」にする（S25）。一方、拡張ヘッダステート情報データSTEHから、拡張ヘッダに誤りが存在する、すなわちMAC構造に誤りが存在することを確認したとき、ステートを「ERR」にする（S24）。拡張ヘッダステート情報データSTEHは拡張ヘッダの各フィールドのステートを示す情報である。

ステートが「HCS_H」のとき、ステートを「HCS_L」にする。ステートが「HCS_L」のとき、ステートを「DA_LD」にする。ステートが「DA_LD」のとき、ステートを「SA_LD」にする。

ステートが「SA_LD」のとき、遅延TEK処理データDDTKの送信先アドレス（DA: Destination Address）と端末装置のアドレスとが一致しているか否かを確認し、一致していないときは、端末装置が処理すべきデータではないので、ステートを「ERR」にする（S26）。そして、一致しているとき、MAC構造がSYNCデータまたはMACMMであるか否か、すなわち、MAC構

造中にMACMMヘッダが存在するか否かを判断し、存在するときはステートを「MAC_MNG」にし、そうでないときはステートを「TL_H」にする（S27）。

ステートが「MAC_MNG」である期間はMACMMヘッダの位置であるため、MACMMヘッダ位置情報データPMMを生成し、これを遅延TEK処理データDDTKとともにMACMMヘッダ解析ブロック24へ送る。MACMMヘッダ解析処理については、後述する。

ステートが「MAC_MNG」であるとき、MACMMヘッダ解析ブロック24の処理が行われている間は、ステートを保持する。そして、MACMMヘッダ解析ブロック24から出力されたMACMMヘッダステート情報データSTMMから、MACMMヘッダ解析処理が正常に終了したことを確認したとき、ステートを「VALID」にする（S29）。一方、MACMMヘッダステート情報データSTMMから、MACMMヘッダに誤りが存在する、すなわちMAC構造に誤りが存在することを確認したとき、ステートを「ERR」にする（S28）。MACMMヘッダステート情報データSTMMはMACMMヘッダの各フィールドのステートを示す情報である。

ステートが「TL_H」のとき、遅延TEK処理データDDTKの送信元アドレス（SA：Source Address）と端末装置のアドレスとが一致しているか否かを確認し、一致しているときは、送信先と送信元が同じであるため不当なデータであると判断し、ステートを「ERR」にし、一致していないときは、ステートを「TL_L」にする（S2A）。ステートが「TL_L」のとき、ステートを「VALID」にする。

ステートが「VALID」のとき、MAC構造の最後のデータが来るまでステートを保持し、MACデータの最後のデータが来たとき、ステートを「FC」にし、次のMAC構造の構造解析を行う（S2B）。

すなわち、MACヘッダ解析ブロック22は、ステートに従った動作の結果、ステートが「EHDR」である期間は拡張ヘッダを示すことから拡張ヘッダ位置情報データPEHを生成し、ステートが「MAC_MNG」である期間はMACMMヘッダを示すことからMACMMヘッダ位置情報データPMMを生成する。

そして、拡張ヘッダステート情報データ STEH と MACMM ヘッダステート情報データ STMM と、MAC ヘッダ解析ブロック 22 で解析した MAC ヘッダのステート情報から、MAC ステート情報データ STMC を生成する。なお、ここで求めたステートと対応させるために、遅延 TEK 処理データ DDTK をさらに遅延させて、構造解析ブロック 20 から出力する。

(MAC ヘッダの誤り検出)

ここでは、HCS チェックによって、MAC ヘッダの誤り検出を行っている。HCS チェックとは、図 7 に示す MAC データの構造における HCS 以外の MAC ヘッダ (FC フィールド、PARM フィールド、LEN フィールド、EHDR フィールド) を CRC 計算し、HCS データと一致比較することによって、MAC ヘッダの誤りを検出する方法である。

図 8 は HCS チェック以外の MAC ヘッダの誤り検出を説明するための図である。同図中、(a) は LEN フィールドのチェック (MAC フレーム長チェック)、(b) は PARM フィールドのチェック (拡張ヘッダ長チェック) を示している。

図 8 (a) に示すように、LEN フィールドのチェックには、LEN フィールド値分カウントする LEN カウンタを用いる。LEN カウンタは、MAC データ先頭位置信号 LPMC が 1 の MAC データ (MAC データ 1) の先頭を示す位置で有効になったとき、カウントをスタートし、次の MAC データ (MAC データ 2) の先頭を示す位置で有効になったとき、そのカウントをストップする。これにより LEN カウンタの値は、MAC データ 1 のデータ長を示すことになり、誤りがなければ、MAC_LEN 長 (= LEN フィールド値 + 6 バイト (FC・PARM・HCS フィールド長に相当)) と一致するはずである。そこで、LEN カウンタの値が MAC_LEN 長と一致するときは、LEN フィールドに誤りがないと判断し、一方、LEN カウンタの値が MAC_LEN 長と一致しないときは、LEN フィールドに誤りがあると判断する。

また図 8 (b) に示すように、PARM フィールドのチェックには、PARM フィールド値分カウントする PARM カウンタを用いる。PARM カウンタは、MAC データ先頭位置信号 LPMC が 1 の MAC データ (MAC データ 3) の先

頭を示す位置で有効になったときから6バイト（FC・PARM・LENフィールド長に相当）進んだ位置から、カウンタをスタートし、PARMフィールド値分カウントした位置でカウンタをストップする。これにより、PARMカウンタがカウンタをストップした位置が拡張ヘッダの終わりに相当することになり、以降、図6に従ったステート解析を進めていく。もし、PARMカウンタが示す拡張ヘッダの最終位置が誤っているときは、以降のステート解析結果はエラーとなる。よってMACデータ3のステート解析が終了した時点で、ステート結果が「ERR」でないときはPARMフィールドに誤りがないと判断し、一方、ステート結果が「ERR」であるときは、PARMフィールドチェックの結果を無視する。

FCフィールドのチェックでは、FCフィールドの値をチェックする処理と、それ以降の図6に従ったステート解析処理が、FCフィールドの値から判断されたデータの種類の適応していることを確認し、ステート結果が「ERR」でないときはFCフィールドに誤りがないと判断し、一方、ステート結果が「ERR」であるときは、FCフィールドチェックの結果を無視する。

EHDRフィールドのチェックでは、後述の拡張ヘッダ解析ブロック23のステート解析結果が「ERR」でないときはEHDRフィールドに誤りがないと判断し、一方、ステート解析結果が「ERR」であるときはEHDRフィールドに誤りがあると判断する。

以上のようにしてMACヘッダの各フィールドをチェックした結果、全てのフィールドについてエラーがない場合は、HCSチェック結果がエラーであった場合であってもMACヘッダに誤りがないと判断する機能を設けることが可能となる。例えば、MACフレーム長チェックおよび拡張ヘッダ長チェックによるチェック結果が、エラーなしであるとき、HCSチェックによるチェック結果を無効にすればよい。なお、このようなMACヘッダの誤り検出方法を用いず、HCSチェックのみによってMACヘッダの誤り検出を行うことも可能である。

<拡張ヘッダ解析>

拡張ヘッダ解析ブロック23は、遅延TEK処理データDDTK中に拡張ヘッダが存在する場合、この拡張ヘッダの解析を行う。具体的には、拡張ヘッダの各

フィールドを逐次チェックし、各フィールドのデータの意味を判断し、データにステートを与える。

図9は拡張ヘッダ解析ブロック23における拡張ヘッダ解析のステートマシンを示す図である。また図10は拡張ヘッダのフォーマットを示す図である。図10に示すように、拡張ヘッダは、拡張ヘッダの種類を示すEH TYPE フィールド、拡張ヘッダのデータ部分を示すEH VALUEフィールド、およびEH VALUEフィールドの長さを示すEH LENフィールドによって構成され、以降、EH TYPE、EH LEN、EH VALUEの各フィールドがセットになって繰り返される。

図9に従って、拡張ヘッダ解析における処理の流れを説明する。ステートマシンのステートは、バイトクロック毎に遷移する。

ステートが初期状態である「IDLE」である場合において、MACヘッダ解析ブロック22から送られた拡張ヘッダ位置情報データPEHが有効であるときは、ステートを「EH_TL」にし、そうでないときはそのステートを保持する(S31)。

ステートが「EH_TL」であるときのMACデータは、拡張ヘッダの種類およびデータ長を示している。拡張ヘッダには、次の3種類がある。すなわち、MACデータの暗号化に関するデータである「Downstream Privacy」、MACデータが連続で送られ、それらが同一ヘッダを有する場合に、繰り返されるヘッダを圧縮し帯域節約を可能にする機能であるPHS (Payload Header Suppression) が施されたデータである「Downstream PHS」、および拡張ヘッダを埋めるために使用される「Null」である。図11は「Downstream Privacy」である拡張ヘッダのフォーマットを示す図である。

ステートが「EH_TL」であるとき、MACデータが上記3種類のいずれかを示しているときは、ステートを「EH_VAL」にし、そうでないときは、遅延TEK処理データDDTKに誤りがあると判断し、ステートを「ERR」にする(S32)。

ステートが「EH_VAL」のとき、拡張ヘッダが「Downstream Privacy」である場合は(S33)、プロトコルのバージョンを示すVersionデータ (Protocol Version Number) の値が0x01でない場合や、EH VALUEフィールドの最後の

データであるReservedデータの値が0 x 0 0でない場合、遅延TEK処理データDDTKに誤りがあると判断して、ステートを「ERR」にする（S34、S35）。

そうでないときは、EH VALUEフィールドが最後であるか否かを確認する（S36）。ここでの確認は、EH LENフィールドの値をカウントするEH LENカウンタによって行う。すなわち、EH LENカウンタの値が、EH LENフィールドの値と一致しないときは、ステートを保持する。一方、一致するときは、拡張ヘッダフィールドの最後であるか否かを確認する（S37）。ここでの確認は、拡張ヘッダ位置情報データPEHを参照して行う。拡張ヘッダフィールドの最後であるときは、拡張ヘッダの解析が正常に終了したと判断し、ステートを「IDLE」にする。そうでないときは、ステートを「EH_TL」にする。

この結果、拡張ヘッダ解析ブロック23は、拡張ヘッダの各フィールドのステート情報、遅延TEK処理データDDTKに誤りがあると判断した場合のエラーステート情報、および拡張ヘッダの解析が正常に終了したと判断した場合の正常終了ステート情報を、拡張ヘッダステート情報データSTE HとしてMACヘッダ解析ブロック22へ出力する。

<MACMMヘッダ解析>

MACMMヘッダ解析ブロック24は、遅延TEK処理データDDTK中にMACMMヘッダが存在する場合、このMACMMヘッダの解析を行う。具体的には、MACMMヘッダの各フィールドを逐次チェックし、各フィールドのデータの意味を判断し、データにステートを与える。

図12はMACMMヘッダ解析ブロック24におけるMACMMヘッダ解析のステートマシンを示す図である。また図13はMACMMヘッダのフォーマットを示す図である。図13において、DAは遅延TEK処理データDDTKの送信先アドレスフィールド、SAは遅延TEK処理データDDTKの送信元アドレスフィールド、Msg LENはMACMMのデータ長フィールド、DSAPはISO 8802-2に準拠したLLC送信先アドレスポイントを示すフィールド、SSAPはISO 8802-2に準拠したLLC送信元アドレスポイントを示すフィールド、Control はISO 8802-3に準拠したUnnumbered 情報フレームフ

フィールド、VersionはMACMMのバージョンを示すフィールド、TypeはMACMMの種類を示すフィールド、RSVDはMAC Management Payloadを32ビット境界上に配置するためのリザーブデータフィールド、MAC Management PayloadはMACMMの実データフィールド、CRCはDAからMAC Management PayloadまでをCRC計算するためのチェックシーケンスデータフィールドである。

図12に従って、MACMMヘッダ解析における処理の流れを説明する。ステートマシンのステートは、バイトクロック毎に遷移する。

ステートが初期状態である「IDLE」である場合において、MACヘッダ解析ブロック22から送られたMACMMヘッダ位置情報データPMMが有効であるときは、ステートを「MSG_L_H」にし、そうでないときはそのステートを保持する(S41)。

ステートが「MSG_L_H」のとき、受信した遅延TEK処理データDDTKの送信元アドレス(SA)と端末装置のアドレスとを比較し、一致しているときは、遅延TEK処理データDDTKが不当なデータであると判断し、ステートを「ERR」にする一方、一致していないときは、ステートを「MSG_L_L」にする(S42)。

ステートが「MSG_L_L」のとき、ステートを「DSAP」にする。ステートが「DSAP」のとき、遅延TEK処理データDDTKの値が0x00であるときは、ステートを「SSAP」にし、そうでないときは、遅延TEK処理データDDTKは不当であると判断し、ステートを「ERR」にする(S43)。

ステートが「SSAP」のとき、遅延TEK処理データDDTKの値が0x00であるときは、ステートを「CONTROL」にし、そうでないときは、遅延TEK処理データDDTKは不当なデータであると判断し、ステートを「ERR」にする(S44)。

ステートが「CONTROL」のとき、遅延TEK処理データDDTKの値が0x03であるときは、ステートを「VERSION」にし、そうでないときは、遅延TEK処理データDDTKは不当なデータであると判断し、ステートを「ERR」にする(S45)。

ステートが「VERSION」のとき、遅延TEK処理データDDTKの値が

0×01または0×02であるときは、ステートを「TYPE」にし、そうでないときは、遅延TEK処理データDDTKは不当なデータであると判断し、ステートを「ERR」にする（S46）。

ステートが「TYPE」のとき、ステートを「RSVD」にする。そして、ステートが「RSVD」のとき、MACMMヘッダ解析が正常に終了したと判断して、ステートを「IDLE」にする。

この結果、MACMMヘッダ解析ブロック24は、MACMMヘッダの各フィールドのステート情報、遅延TEK処理データDDTKに誤りがあると判断した場合のエラーステート情報、およびMACMMヘッダの解析が正常に終了したと判断した場合の正常終了ステート情報を、MACMMヘッダステート情報データSTMMとしてMACヘッダ解析ブロック22へ出力する。

MACヘッダ解析ブロック22、拡張ヘッダ解析ブロック23およびMACMMヘッダ解析ブロック24の処理をもって、構造解析ブロック20の処理が終了する。処理の終了後、MACステート情報データSTMCと、これに対応する遅延TEK処理データDDTKとが、復号ブロック30に送られる。

<復号ブロック>

復号ブロック30は、構造解析ブロック20から出力された遅延TEK処理データDDTKおよびMACステート情報データSTMCを入力とし、遅延TEK処理データDDTKにおいて、データの機密性保護のためセンター装置側でDES（Data Encryption Standard）により暗号化された部分のデータについて復号処理を行い、その処理結果をTEK処理結果データRTEKとしてデータ記憶装置14に出力する。

図14は復号ブロック30の動作を示すフローチャートである。図14において、31は遅延TEK処理データDDTKおよびMACステート情報データSTMCを入力とし、遅延TEK処理データDDTKの暗号の有無を判別し、第1の復号処理対象データDD1および復号処理対象外データDDXを出力する暗号有無チェックブロック、32は第1の復号処理対象データDD1を復号処理に適応したビット幅である64ビットに変換し、第2の復号処理対象データDD2として出力する第1のビット変換ブロックである。33は遅延TEK処理データDD

TEKから、TEKデータTEKを選択するためのTEK照合データITEKを抽出するTEK照合データ抽出ブロック、34はTEK照合データITEKを用いてTEKデータTEKを抽出するTEKデータ抽出ブロックである。35は第2の復号処理対象データDD2に対して復号処理を行い、第1の復号処理結果データRD1を出力する復号処理ブロック、36は第1の復号処理結果データRD1を復号処理対象外データDDXと同一ビット幅である8ビットに変換し、第2の復号処理結果データRD2として出力する第2のビット変換ブロック、37は第2の復号処理結果データRD2と復号処理対象外データDDXとを結合し、結合データCBDとして出力するデータ結合ブロック、38は結合データCBDをデータ記憶装置14に適応したビット幅に変換し、TEK処理結果データRTEKとして出力する第3のビット変換ブロックである。

ここで、第1の復号処理対象データDD1は遅延TEK処理データDDTK中のDES暗号処理化された部分のデータであり、復号処理対象外データDDXは遅延TEK処理データDDTK中のDES暗号処理化されていない部分のデータである。またTEKデータTEKは暗号を解くためのデータであり、ここでは実際にデータの暗号化および復号化に使用するDES暗号キーである。TEK照合データITEKは、予め保持していた複数のTEKデータの中から復号に用いるTEKデータTEKを選択するために照合するシーケンスデータである。ここでは、TEKデータTEKは復号処理の初期値データを含むものとする。

なお、TEKデータは解読防止のために定期的に変更されるので、TEKデータが更新される際にセンター装置と端末装置との間の通信が途切れないように、TEKデータ抽出ブロック34に、前後のTEKデータ、復号処理の初期値データ、および遅延TEK処理データDDTK中の拡張ヘッダに設定されたTEKデータのインデックス・シーケンス番号を予め格納するデータ記憶バッファを設けておく。

以下、図14に従って、復号ブロック30の処理について説明する。なお、MACステート情報データSTMCMは、少なくとも、拡張ヘッダに含まれたMACデータが暗号化されているか否かを示すEncryptビットから生成されるMACデータEncrypt信号と、MACヘッダおよびアドレスデータ(SA, DA)の位置

を示すイネーブル信号と、拡張ヘッダに存在するTEK照合データの位置を示すTEK照合データイネーブル信号とを、含むものとする。

まず暗号有無チェックブロック31において、MACステート情報データSTMCを参照して、遅延TEK処理データDDTK中の暗号化された部分と暗号化されていない部分とを判別し、第1の復号処理対象データDD1および復号処理対象外データDDXを出力する。すなわち、MACデータEncrypt 信号が、MACデータが暗号化されていることを示している場合、MACデータ中のMACヘッダおよびアドレスデータを復号処理対象外データDDXとして出力するとともに、それ以外のMACデータを第1の復号処理対象データDD1として出力する。一方、MACデータEncrypt 信号が、MACデータが暗号化されていない場合、MACデータ全体を復号処理対象外データDDXとして出力する。

その後、第1の復号処理対象データDD1は、第1のビット変換ブロック32において、復号処理単位のビット幅である64ビットに変換され、第2の復号処理対象データDD2として出力される。

また、TEK照合データ抽出ブロック33において、遅延TEK処理データDDTKから、TEKデータを選択するためのTEK照合データITEKを抽出する。すなわち、TEK照合データイネーブル信号が示すデータを、TEK照合データITEKとして抽出して出力する。そして、TEKデータ抽出ブロック34において、TEK照合データITEKを用いて、データ記憶バッファからTEKデータTEKを抽出する。

その後、復号処理ブロック35において、第2の復号処理対象データDD2およびTEKデータTEKを用いて復号処理を行い、当該処理の結果を第1の復号処理結果データRD1とする。

次に、第2のビット変換ブロック36において、第1の復号処理結果データRD1を復号処理対象外データDDXと同一ビット幅である8ビットに変換し、この変換結果を第2の復号処理結果データRD2として出力する。そして、データ結合ブロック37において、第2の復号処理結果データRD2と復号処理対象外データDDXとを統合し、結合データCBDとして出力した後、第3のビット変

換ブロック 38において、結合データ CBD をデータ記憶装置 14 に適応したビット幅に変換し、当該処理の結果を TEK 処理結果データ RTEK としてデータ記憶装置 14 へ出力する。

なお、復号処理単位である 64 ビット、および第 2 の復号処理結果データ RD 2 のビット幅である 8 ビットは、その値に限られるものではなく、例えば $8 \times n$ (n : 整数) ビットで自由に選択可能である。

以上のように本発明によると、センター装置および複数の端末装置によって構成される双方向通信網におけるデジタル双方向通信制御装置において、MAC 機能の中でも演算処理量の大きい TEK 機能の専用処理を、CPU とは別の TEK 処理ブロックによって実行させる。これにより、CPU の負荷を低減することができるとともに、回路規模の適正化が可能となり、さらにスループットが向上するので、装置全体としてのコストパフォーマンスを高めることができる。

請求の範囲

1. デジタル双方向通信における双方向制御を行う装置であって、
入力されたダウンストリームデータをフォーマット変換して、下り方向データを生成するインターフェースブロックと、
前記下り方向データを受けて、MAC (Media Access Control) 機能を実現するCPUと、
前記下り方向データから得られたTEK (Traffic Encryption Key) 処理データを受け、そのデータ構造の解析を行い、この解析結果を基にして、復号処理を行うTEK処理ブロックとを備えた
ことを特徴とするデジタル双方向通信制御装置。
2. 請求項1において、
前記TEK処理ブロックは、
TEK処理データを入力し、このTEK処理データの中のMPEG構造と、MPEG構造に埋め込まれたMAC (Media Access Control) 構造とを解析し、MAC構造を持つデータであるMACデータの状態および意味を示すMACステート情報データを出力する構造解析ブロックと、
TEK処理データ中の暗号化された部分を、前記MACステート情報データを参照して判別し、暗号化された部分を、暗号を解くためのTEKデータを用いて復号し、その復号結果を暗号化されていない部分と統合する復号ブロックとを備えたものである
ことを特徴とするデジタル双方向通信制御装置。
3. 請求項2において、
前記構造解析ブロックは、
TEK処理データ中のMPEG構造のヘッダであるMPEGヘッダを解析し、MACデータの位置を示すMACデータ位置信号、およびMACフレームの先頭バイト位置を示すMACデータ先頭位置信号を出力するMPEGヘッダ解析ブロックと、

前記MACデータ位置信号およびMACデータ先頭位置信号を入力とし、MAC構造のヘッダであるMACヘッダ中の拡張ヘッダおよびMACMM (MAC Management Message) ヘッダ以外のフィールドについて、ステート情報を認識するとともに、TEK処理データに拡張ヘッダが存在するとき、拡張ヘッダの位置を示す拡張ヘッダ位置情報データを出力し、かつ、TEK処理データにMACMMヘッダが存在するとき、MACMMヘッダの位置を示すMACMMヘッダ位置情報データを出力するMACヘッダ解析ブロックと、

前記拡張ヘッダ位置情報データを受けて、拡張ヘッダの各フィールドをチェックし、拡張ヘッダのステート情報を示す拡張ヘッダステート情報データを出力する拡張ヘッダ解析ブロックと、

前記MACMMヘッダ位置情報データを受けて、MACMMヘッダの各フィールドをチェックし、MACMMヘッダのステート情報を示すMACMMヘッダステート情報データを出力するMACMMヘッダ解析ブロックとを備え、

前記MACヘッダ解析ブロックは、

前記拡張ヘッダステート情報データおよびMACMMヘッダステート情報データを受け、MACヘッダ中の拡張ヘッダおよびMACMMヘッダ以外の各フィールドのステート情報と、前記拡張ヘッダステート情報データが示す拡張ヘッダのステート情報、および前記MACMMヘッダステート情報データが示すMACMMヘッダのステート情報とを基にして、前記MACステート情報データを生成するものである

ことを特徴とするデジタル双方向通信制御装置。

4. 請求項3において、

前記MPEGヘッダ解析ブロックは、

MPEGヘッダのフィールドをチェックして、MACデータの位置とMACフレームの先頭バイト位置とを検出し、前記MACデータ位置信号およびMACデータ先頭位置信号を出力するものである

ことを特徴とするデジタル双方向通信制御装置。

5. 請求項3において、

前記MACヘッダ解析ブロックは、

HCSチェックによって、MACヘッダの誤り検出を行うものである
ことを特徴とするデジタル双方向通信制御装置。

6. 請求項3において、

前記MACヘッダ解析ブロックは、

MACヘッダの中のMACデータ長を示すフィールドのチェックを行うもので
あり、

前記チェックを、前記MACデータ先頭位置信号を参照してMACフレームの
データ長をカウントし、このMACフレーム長が、当該フィールドの値と所定の
データ長との和と一致するか否かを判断することによって、行う
ことを特徴とするデジタル双方向通信制御装置。

7. 請求項3において、

前記MACヘッダ解析ブロックは、

HCSチェックに加えて、MACフレーム長チェックおよび拡張ヘッダ長チェ
ックによって、MACヘッダの誤り検出を行うものであり、かつ、

前記MACフレーム長チェックおよび拡張ヘッダ長チェックによるチェック結
果が、エラーなしであるとき、前記HCSチェックによるチェック結果を無効に
する

ことを特徴とするデジタル双方向通信制御装置。

8. 請求項3において、

前記拡張ヘッダ解析ブロックは、

前記拡張ヘッダ位置情報データを参照して、拡張ヘッダのフィールドをチェ
ックし、拡張ヘッダのデータ長や種類を判別し、

拡張ヘッダのフィールドの値が不当である場合、拡張ヘッダに誤りがあると認
識し、その旨を、前記拡張ヘッダステート情報データとして出力するものである

ことを特徴とするデジタル双方向通信制御装置。

9. 請求項3において、

前記MACMMヘッダ解析ブロックは、

前記MACMMヘッダ位置情報データを参照して、MACMMヘッダのフィールドをチェックし、MACMMのデータ長および種類を判別し、

MACMMヘッダのフィールドのデータの値が不当である場合、MACMMヘッダに誤りがあると認識し、その旨を、前記MACMMヘッダステート情報データとして出力するものである

ことを特徴とするデジタル双方向通信制御装置。

10. 請求項2において、

前記復号ブロックは、

前記MACステート情報データを参照して、TEK処理データ中の、暗号化された部分と暗号化されていない部分とを選別し、

TEK処理データから、TEKデータを選択するためのTEK照合データを抽出し、

抽出したTEK照合データを参照して、予め保持していた複数のTEKデータの中から、復号に用いるTEKデータを選択し、

暗号化された部分を復号処理単位のビット幅に変換し、選択したTEKデータを用いて、復号し、

復号後のデータと、暗号化されていない部分とを統合するものである

ことを特徴とするデジタル双方向通信制御装置。

11. デジタル双方向通信における双方向制御を行う方法であって、

入力されたダウンストリームデータをフォーマット変換して、下り方向データを生成するステップと、

CPUによって、前記下り方向データを受けて、MAC(Media Access Control)機能を実現するステップと、

TEL 処理ブロックによって、前記下り方向データから得られた TEK (Traffic Encryption Key) 処理データを受け、そのデータ構造の解析を行い、この解析結果を基にして、復号処理を行う TEK 処理ステップとを備えたことを特徴とするデジタル双方向通信制御方法。

12. 請求項 11 において、

前記 TEK 処理ステップは、

TEK 処理データの中の MPEG 構造と、MPEG 構造に埋め込まれた MAC (Media Access Control) 構造とを解析し、MAC 構造を持つデータである MAC データの状態および意味を示す MAC ステート情報データを生成する構造解析ステップと、

TEK 処理データ中の暗号化された部分を、前記 MAC ステート情報データを参照して判別し、暗号化された部分を、暗号を解くための TEK データを用いて復号し、その復号結果を暗号化されていない部分と統合する復号ステップとを備えたものである

ことを特徴とするデジタル双方向通信制御方法。

13. 請求項 12 において、

前記構造解析ステップは、

TEK 処理データの MPEG 構造のヘッダである MPEG ヘッダを解析し、MAC データの位置を示す MAC データ位置信号、および MAC フレームの先頭バイト位置を示す MAC データ先頭位置信号を生成する MPEG ヘッダ解析ステップと、

前記 MAC データ位置信号および MAC データ先頭位置信号を用い、MAC 構造のヘッダである MAC ヘッダ中の拡張ヘッダおよび MAC MM (MAC Management Message) ヘッダ以外のフィールドについて、ステート情報を認識するとともに、TEK 処理データに拡張ヘッダが存在するとき、拡張ヘッダの位置を示す拡張ヘッダ位置情報データを生成し、かつ、TEK 処理データに MAC MM ヘッダが存在するとき、MAC MM ヘッダの位置を示す MAC MM ヘッダ位置情報デー

タを生成するMACヘッダ解析ステップと、

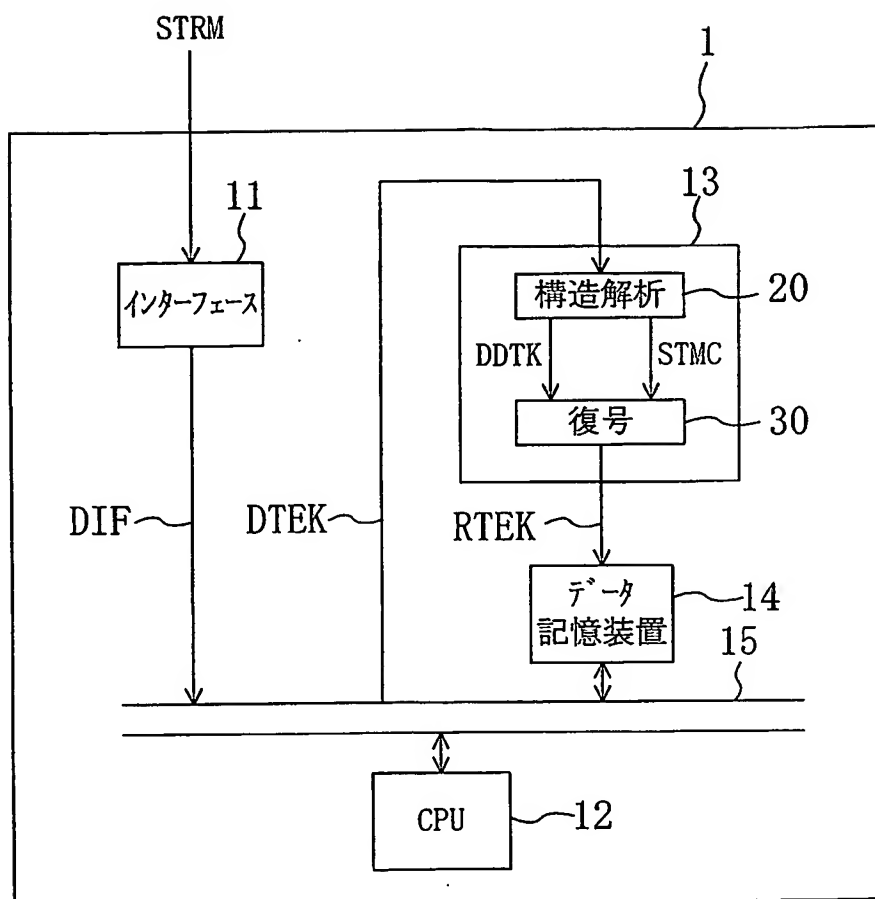
前記拡張ヘッダ位置情報データを受けて、拡張ヘッダの各フィールドをチェックし、拡張ヘッダのステート情報を示す拡張ヘッダステート情報データを生成する拡張ヘッダ解析ステップと、

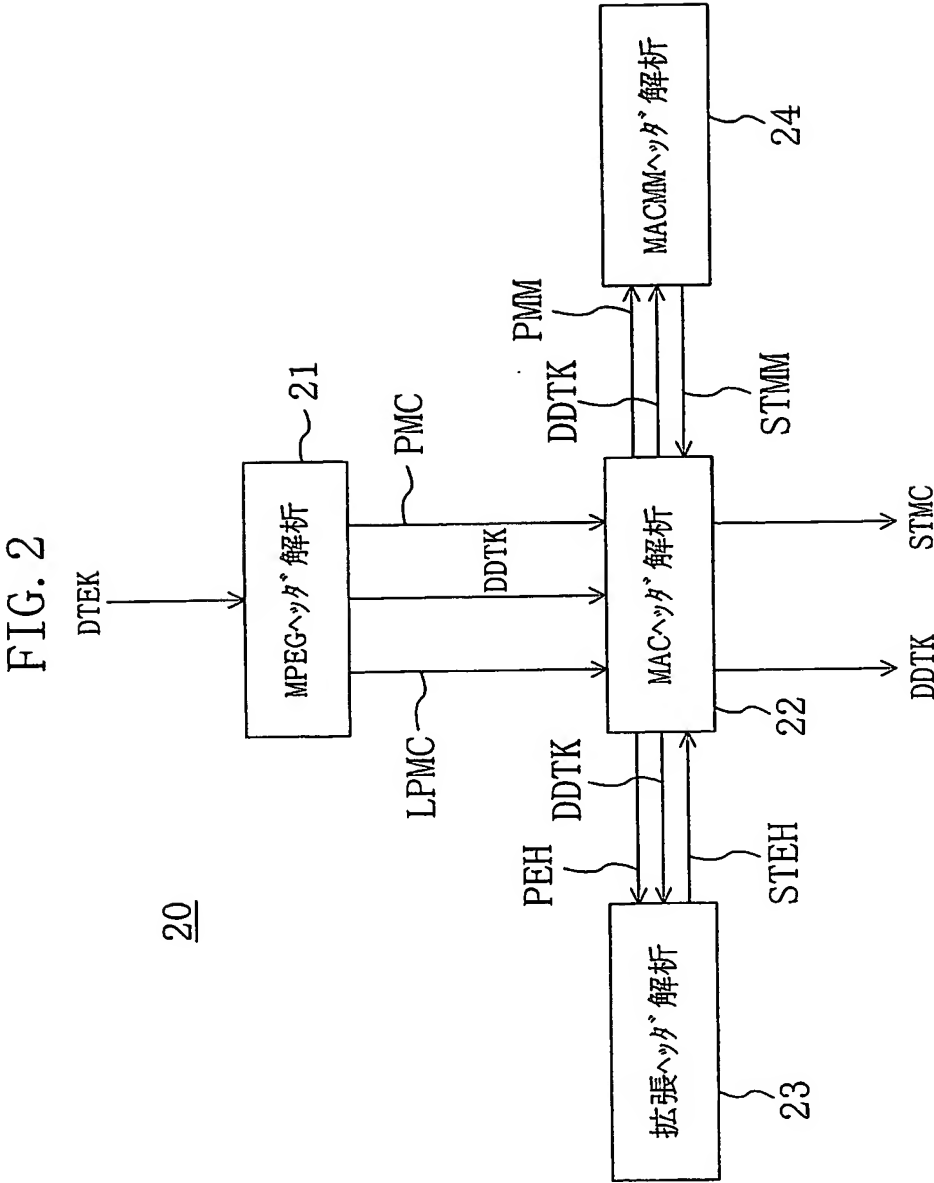
MACMMヘッダ位置情報データを受けて、MACMMヘッダの各フィールドをチェックし、MACMMヘッダのステート情報を示すMACMMヘッダステート情報データを生成するMACMMヘッダ解析ステップとを備え、

前記MACヘッダ解析ステップにおいて判断した、MACヘッダ中の拡張ヘッダおよびMACMMヘッダ以外の各フィールドのステート情報と、前記拡張ヘッダステート情報データが示す拡張ヘッダのステート情報、および前記MACMMヘッダステート情報データが示すMACMMヘッダのステート情報とを基にして、前記MACステート情報データを生成するものであることを特徴とするデジタル双方向通信制御方法。

1/14

FIG. 1





3/14

FIG. 3

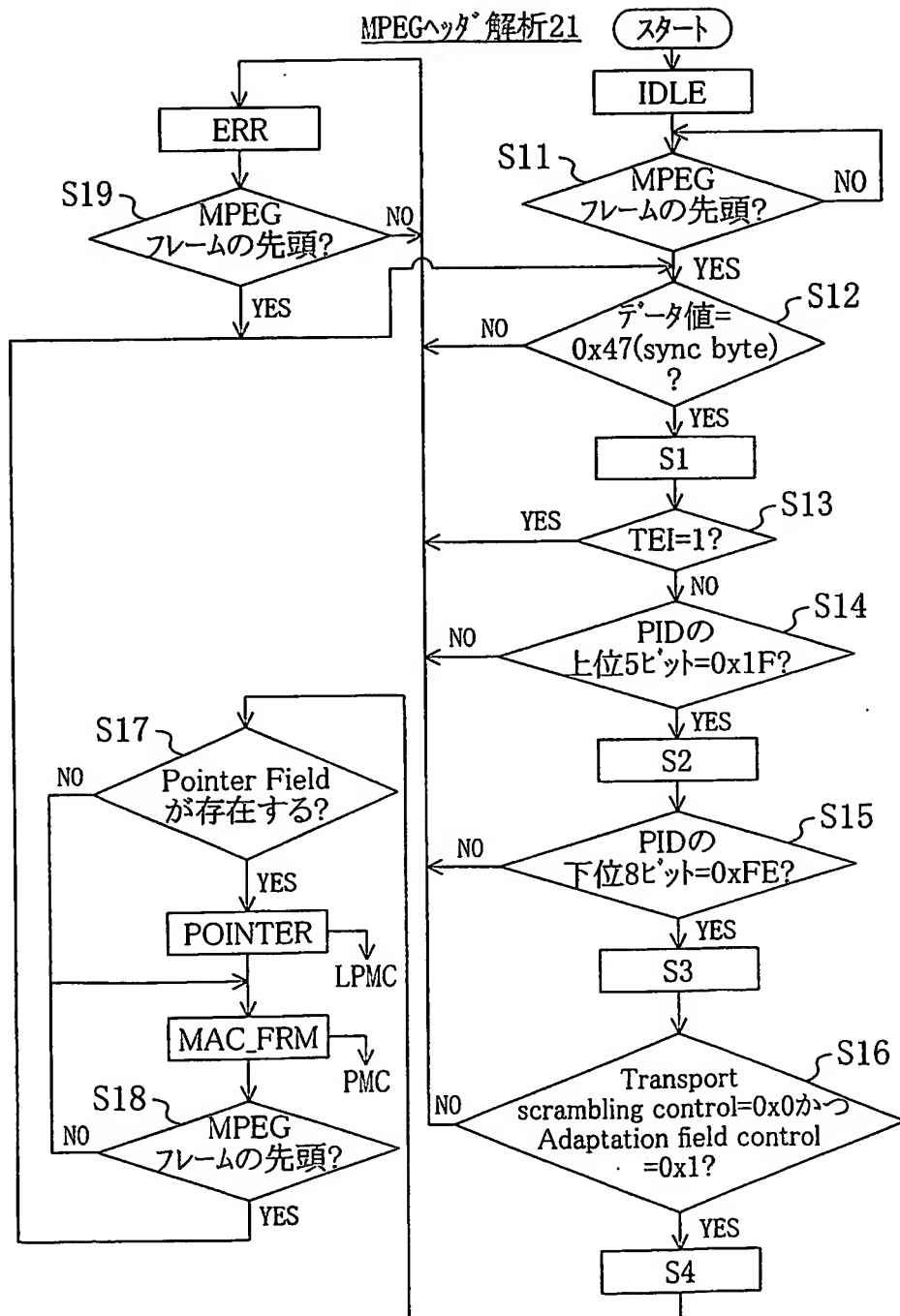


FIG. 4

Field	Length (bit)	Description
sync byte	8	0x47:MPEG Packet Sync Byte
transport error indicator (TEI)	1	0...パケットにエラーがない場合 1...パケットにエラーがある場合
payload unit start indicator (PUSI)	1	0...pointer fieldがない場合 1...pointer fieldがある場合 *pointer fieldはMPEGフレームの5バイト目 PUSIはそのパケットにペイロードのスタートがある場合に立つ
transport priority	1	0(予約)
PID	13	DOCSIS Data-Over-Cableの場合は0x1FFE
transport scrambling control	2	0(予約)
adaptation field control	2	1(DOCSIS PIDではこのフィールドの使用は不可)
continuity counter	4	PIDの循環カウンタ

FIG. 5

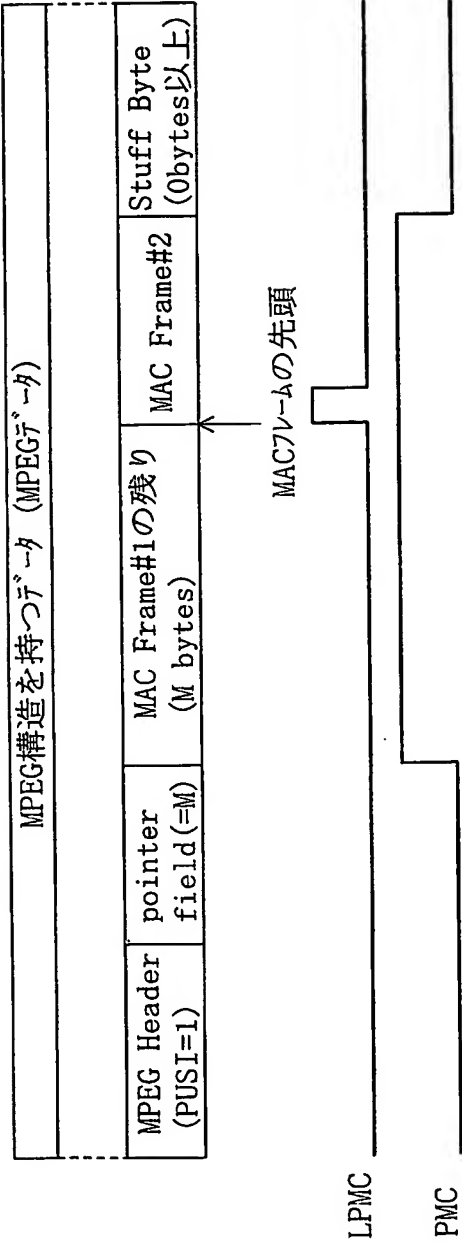


FIG. 6

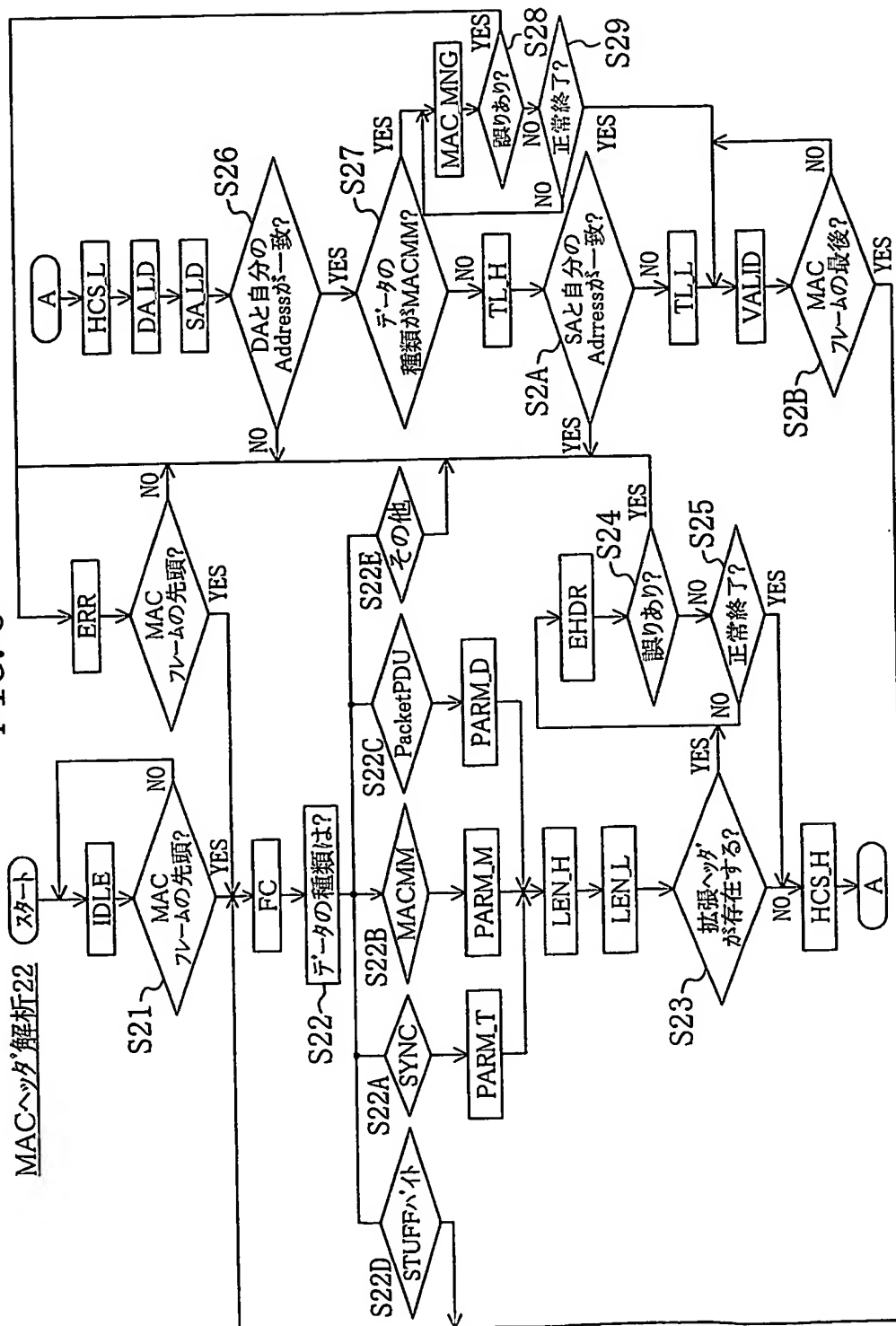
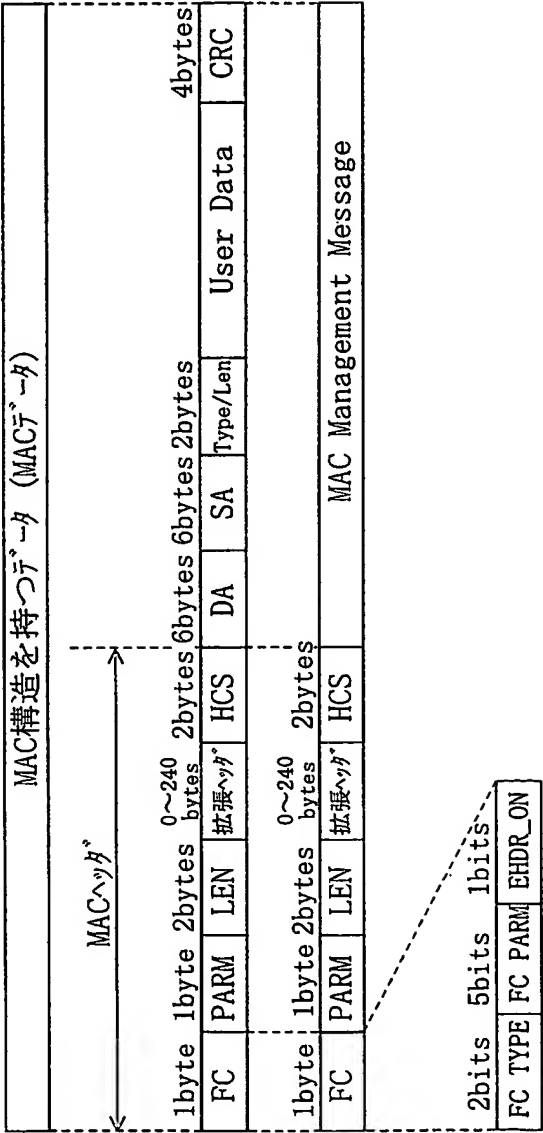


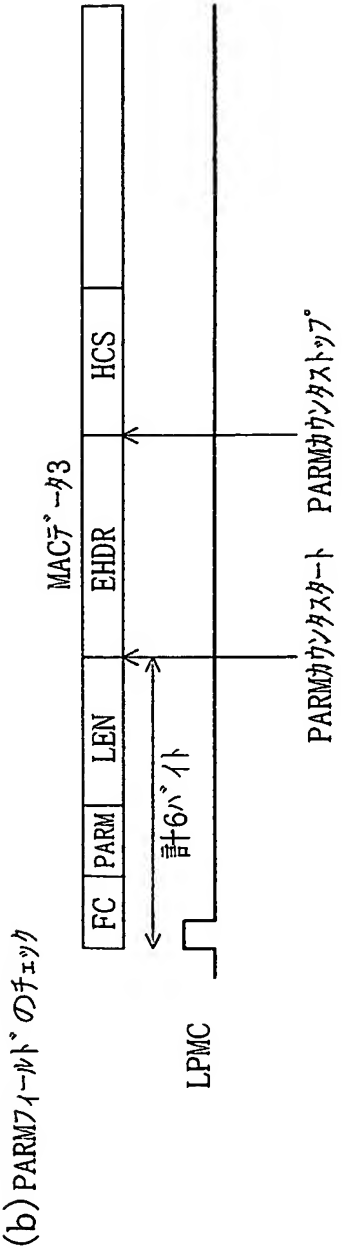
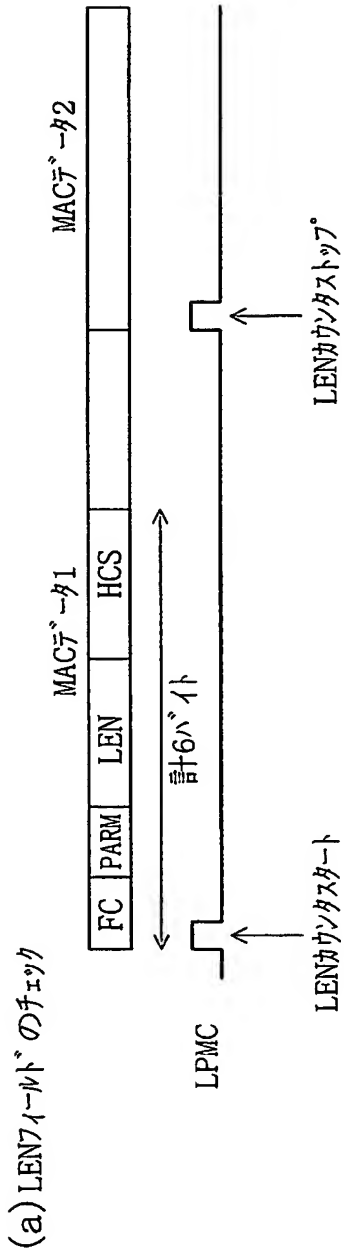
FIG. 7



Packet PDU
の場合

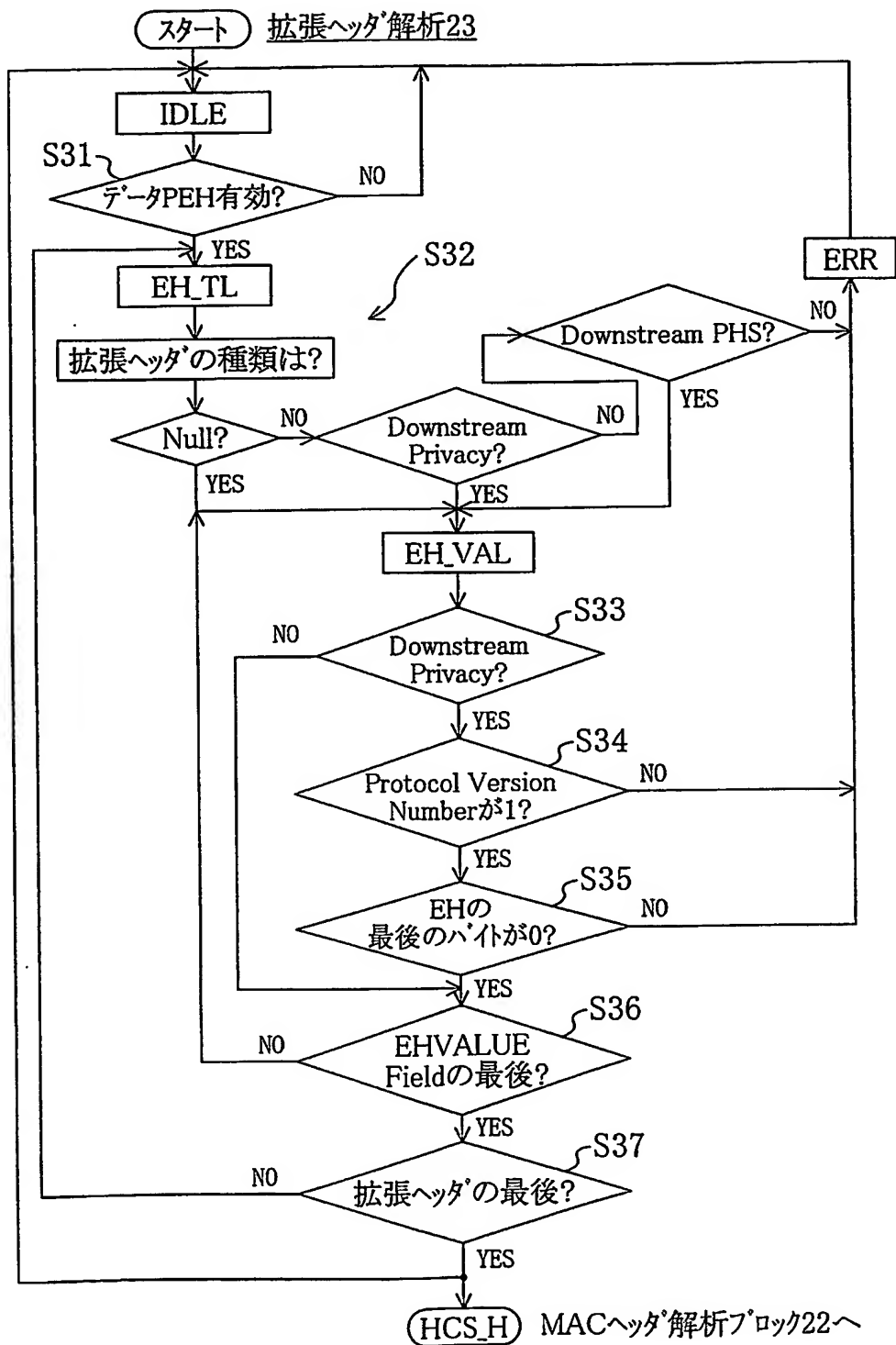
SYNCおよび
MACMMの場合

FIG. 8



9/14

FIG. 9



差替え用紙 (規則26)

FIG. 10

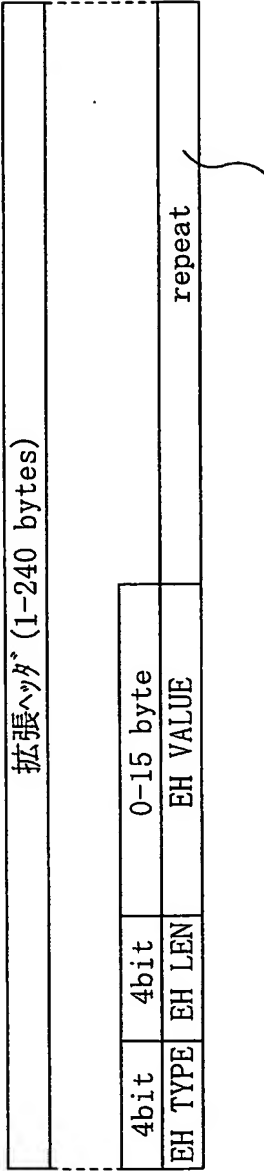


FIG. 11

拡張ヘッダ (Downstream Privacy)					
1byte	1byte	2bytes		1byte	
Type=4	LEN=4	KEY_SEQ	Version=1	E	T
		SID		Reserved=0	

FIG. 12

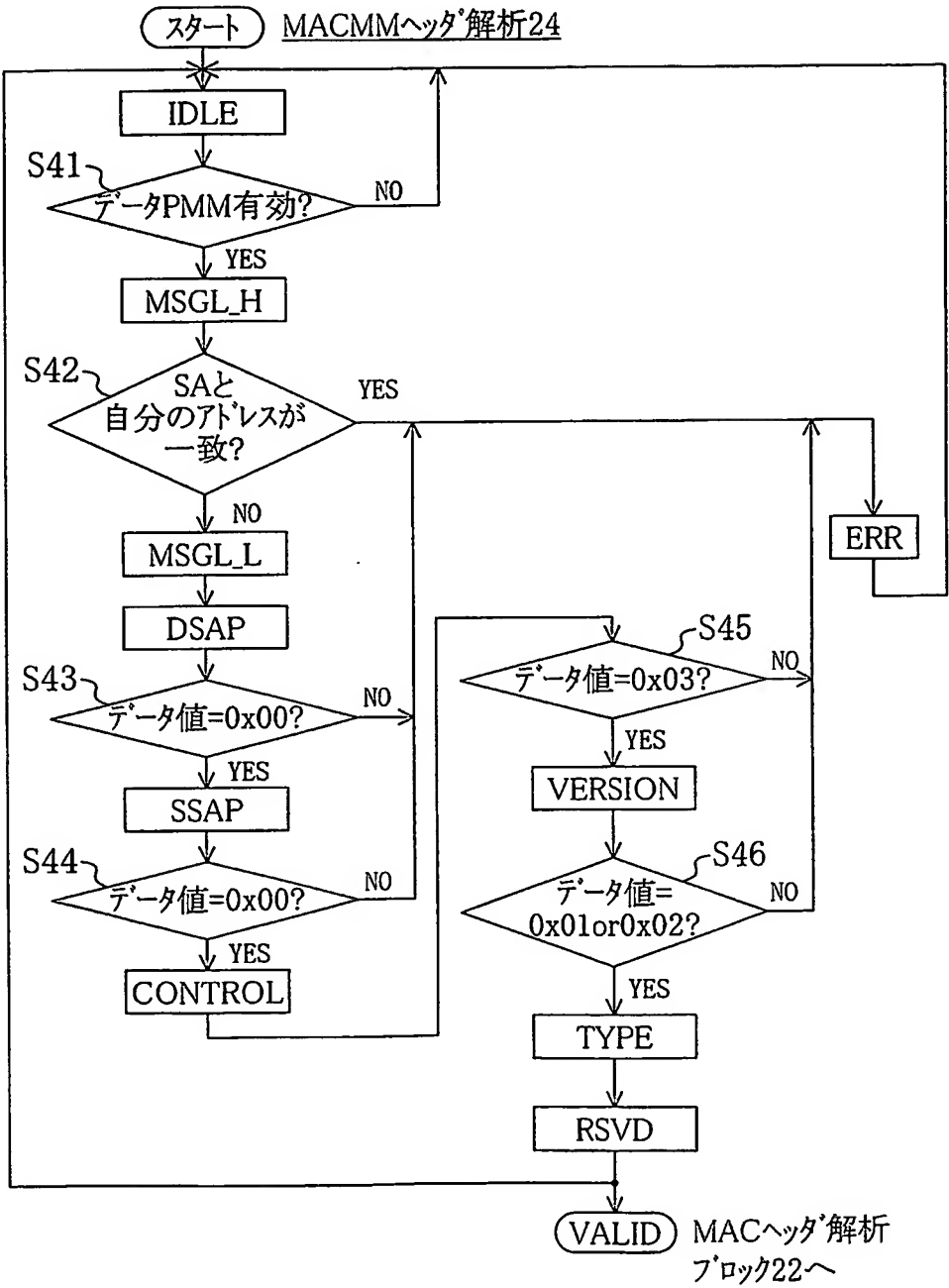
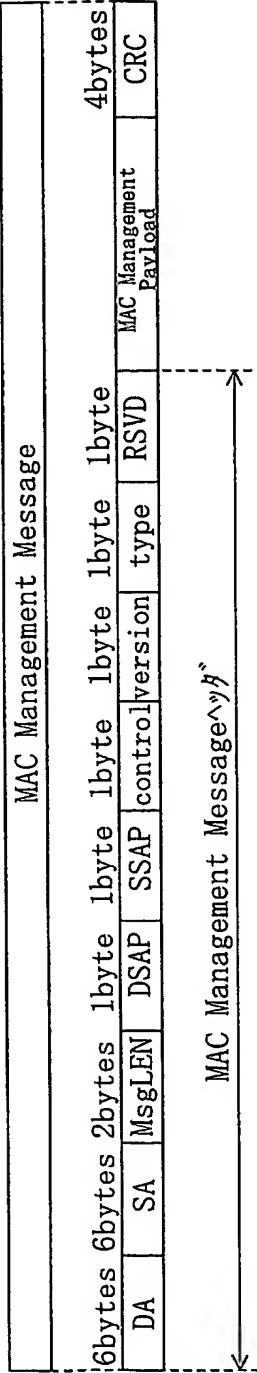


FIG. 13



14/14

FIG. 14

